Notice of Allowability	Application No.	Applicant(s)	
	09/827,227	MACKENZIE, PHILIP D.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *1/23/06*.

2. ☒ The allowed claim(s) is/are *1-20*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

1. This is in response to the arguments filed on 23 January 2006.

2. Claims 1-20 are pending in the application.

3. Claims 1-20 have been allowed.

Response to Arguments

4. Applicant's arguments, see pages 2 and 3, filed 23 January 2006, with respect to claims 1-20 have been fully considered and are persuasive. The rejection of the claims has been withdrawn.

Allowable Subject Matter

5. Claims 1-20 are allowed.

The following is an examiner's statement of reasons for allowance:

The present invention is directed towards a method for communication via a data network, between two parties that share a password, using a Diffie-Hellman type key exchange on a particular group to generate a shared secret g^{xy}, where g is the group generator known to both parties and x is an index known to one party and y is an index known to the other party, the group having a group operation and an inverse group operation. The method comprises the steps of one party generating a parameter m by performing the group operation on g^x and a function of at least the password, wherein any portion of a result associated with the function that is outside the group is randomized, and transmitting m to the other party, whereby the other party may perform the inverse group operation on m and the function of at least the password, and remove the randomization of any portion of the result associated with the function that is outside the group, to extract g^x and calculate the shared secret g^{xy}. Independent claims 10 and 19 recite similar limitations in accordance with apparatus and article of manufacture aspects of the

invention. Independent claims 8, 17 and 20 respectively recite similar limitations as claims 1, 10 and 19 from the perspective of the "other party".

The closest prior art to the current application was Wu U.S. Patent No. 6,539,479 B1 (hereinafter Wu). While Wu is a password-only authentication protocol, Wu does not teach or suggest each and every element of the claimed invention. Wu does not teach or suggest "any portion of a result associated with the function that is outside the group is randomized... and remov[ing] the randomization of any portion of the result associated with the function that is outside the group," as recited in the claimed invention. Wu does not teach or suggest randomizing the part of a result lying outside a group and subsequently removing that randomization. The only randomness that Wu discloses is when client computer ("Carol," as referred to in Wu) generates a random number, for example, w_s (in the log-in procedure of FIG. 2), and the server ("Steve," as referred to in Wu) generates a random number u, from which the server attempts to authenticate the client computer, see column 8, lines 43 through column 9 line 15. Columns 10 through 12 of Wu describe variants of the protocol. However, again, the only randomness is with respect to certain values generated by either the server (e.g., random string r_1 in step 210A) or the client computer (e.g., random string r_2 in step 230). Thus, in Wu, there is no notion of any result being "outside of a group". Hence, it is not possible for Wu to disclose randomizing something outside of a group. Therefore, it is quite clear that Wu fails to teach or suggest "any portion of a result associated with the function that is outside the group is randomized... and remov[ing] the randomization of any portion of the result associated with the function that is outside the group," as recited in the claimed invention.

For the reasons stated above, the examiner asserts that claims 1, 3-8, 10, 12-17, 19 and 20 are patentable over Wu. Any claims not explicitly allowed are allowed on the virtue of their dependency.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy AM
February 1, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100